Divisibilidad. Números primos. Congruencia

Título: Divisibilidad. Números primos. Congruencia. **Target:** Profesores de Matemáticas.. **Asignatura:** Matemáticas..
Autor: Emiliana Oliván Calzada, Licenciada en Matemáticas, Profesora de Matemáticas en Educación Secundaria.

Comenzaremos este artículo con el concepto de división euclídea o entera.

Proposición: Dados $a,b \in Z \; con \; b \neq 0 \Rightarrow \exists c,r \in Z \; tal \; que \; a = b \cdot c + r \; con \; |r| < |b|$.

Definición:

Se llama ***división euclídea ó entera*** a la operación consistente en calcular los dos números c y r que verifican la proposición anterior, llamados respectivamente cociente y resto.

Observación: A diferencia de la división en el conjunto de los números naturales, en el conjunto de los números enteros el resultado no es único, en general existen dos resultados uno por defecto y otro por exceso.

Ejemplo: $29 = 7 \cdot 4 + 1$ (el cociente es por defecto)

$29 = 8 \cdot 4 + (-3)$ (el cociente es por exceso)

Podemos obtener unicidad en el resultado, imponiendo el signo del resto.

1. *DIVISIBILIDAD EN* Z

Definición: Dados dos números enteros a y b se dice que a es ***divisor*** de b (y se escribe $a|b$) si $\exists c \in Z$ con $b = a \cdot c$. En este caso también se dice que b es ***divisible*** por a ó que b es ***múltiplo*** de a (que denotamos como $b = \dot{a}$).

Propiedades:

a) Si $0|b$ necesariamente $b = 0$.

b) Propiedad reflexiva: $\forall b \in Z : b|b, \; 1|b, \; -1|b, \; -b|b$.

c) Propiedad antisimétrica: Si $a|b \; y \; b|a$ se concluye que $a = b$ ó $a = -b$

d) Propiedad transitiva: Si $a|b \ y \ b|c$, entonces $a|c$

e) Si $b|1$, entonces $b=1 \ ó \ b=-1$

f) Cualquier número es divisor de cero: $\forall a \in Z : a|0$.

g) Si $a|b \ y \ a|c$, entonces $a|b+c \ y \ a|b-c$.

h) Siempre se tiene que $b|b \cdot c$.

i) Si $a|b$, entonces $a|b \cdot c$.

j) $a|b \Leftrightarrow a|-b$.

k) Si $a|b$ y $b \neq 0$, entonces: $|a| \leq |b|$.

Observaciones:

- Dado un número entero $a \neq 0$, el conjunto de todos sus divisores, que denotaremos $D(a)$ está formado por un número finito de elementos.
- Cualquier número entero es divisible por 1, por -1, por sí mismo y por su opuesto.

Definición: Se dice que un número entero a es ***primo***, si tiene exactamente cuatro divisores, es decir, $D(a)=\{1,-1,a,-a\}$.

Notas:

- $a \ es \ primo \Leftrightarrow -a \ es \ primo$ (ya que tienen los mismos divisores).
- $0,1,-1$ no son números primos porque no tienen cuatro divisores.

Teorema (de Euclides)

Sean $a,b \in Z$, tales que p es primo y que $p|a \cdot b$. Entonces: $p|a \ \ ó \ \ p|b$.

Demostración:

Sea $H=\{p\cdot m+a\cdot n \mid m,n\in Z \ y \ p\cdot m+a\cdot n\neq 0\}$.

Sea $k\in H$ con valor absoluto mínimo entre los elementos de H.

$k\neq 0\Rightarrow \exists c,r\in Z \ tal \ que \ a=c\cdot k+r \ \ y \ \ |r|<|k|$. Entonces: $r=a-c\cdot k$.

Como k es de la forma $p\cdot m+a\cdot n$, entonces vemos que

$r=a-c\cdot k=a-c\cdot(p\cdot m+a\cdot n)=a\cdot(1-c\cdot n)+p\cdot(-m\cdot c)=a\cdot n'+p\cdot m'$ es de la misma forma.

Como k es de valor absoluto mínimo de H y $|r|<|k|\Rightarrow r\notin H$

$\overset{r=an'+pm'}{\Rightarrow} \ \ r=0\Rightarrow a=c\cdot k\Rightarrow k \ es \ divisor \ de \ a\Rightarrow k\mid a$.

Análogamente se demuestra que k es divisor de p. Y como p es primo, entonces: $k=1,-1,p,-p$.

- Si $k=p,-p$ tenemos que $p\mid k$ y como $k\mid a \overset{Transitiva}{\Rightarrow} p\mid a$
- En caso contrario tenemos que $1=p\cdot m+a\cdot n$. Entonces:

$$\left.\begin{array}{l} p\mid b\cdot p\cdot m \\ p\mid b\cdot a\Rightarrow p\mid b\cdot a\cdot n \end{array}\right\}\Rightarrow p\mid b\cdot p\cdot m+b\cdot a\cdot n\Rightarrow p\mid b\cdot(pm+an)=b\cdot 1=b\Rightarrow p\mid b$$

Proposición: Sea a un número entero distinto de $0,1,-1$. Entonces a es primo o producto de primos.

Demostración: Por inducción sobre el valor absoluto de a.

- Si $|a|=2\Rightarrow a=2 \ \ ó \ \ a=-2$ que son números primos.
- Supongamos el resultado cierto para cualquier número entero que tenga valor absoluto menor que $|a|$.
- Si a es primo el resultado es cierto.

Si a no es primo $\Rightarrow \exists m \mid a \ \ con \ \ m \neq a, -a, 1, -1.$

$$m \mid a \Rightarrow \exists n \in Z \ tal \ que \ \ a = m \cdot n \Rightarrow |a| = |m| \cdot |n| \Big\} \Rightarrow |n| \neq 1, |a|$$
$$m \neq a, -a, 1, -1 \Rightarrow |m| \neq 1, |a|$$

Luego m, n tienen valor absoluto menor que el de $a \overset{\text{Hioótesis de Inducción}}{\Rightarrow}$ ambos pueden ponerse como producto de números primos, o son primos.

$$m = p_1 \cdot p_2 \cdots p_k; \ \ n = q_1 \cdot q_2 \cdots q_s \quad con \quad p_i, q_j \ \ primos$$
$$\rightarrow a = m \cdot n = p_1 \cdot p_2 \cdots p_k \cdot q_1 \cdot q_2 \cdots q_s$$, que es producto de número primos.

Proposición: La descomposición en factores primos de un número entero es única (salvo cambios de signo de los factores).

Demostración: Sea a un número que no es primo, ya que si a es número primo es trivial.

Sea $a = p_1 \cdots p_r = q_1 \cdots q_k$. Entonces: $p_1 \mid a = q_1 \cdots q_k \overset{\text{Tma de Euclides}}{\Rightarrow} p_1 \mid q_i$ para algún i.

q_i es primo $\Rightarrow p_1 = 1, -1, q_i, -q_i$. Como 1 y -1 no son primos, necesariamente $p_1 = q_i, -q_i$, con lo que podemos eliminar estos dos factores y repetir el proceso.

Consecuencia: Cualquier número entero puede ponerse de manera única en la forma $a = \alpha \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ donde $\alpha = \pm 1$ y $p_1, \cdots, p_k$ son números primos positivos.

Observación: Sean $a = \alpha \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$ y $b = \beta \cdot p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$ donde si algún factor p_i primo no aparece en las factorizaciones de a o de b, se representa con exponente cero. Entonces $b \mid a \Leftrightarrow n_1 \geq m_1; \cdots; n_k \geq m_k$.

2. MÁXIMO COMÚN DIVISOR Y MÍNIMO COMÚN MÚLTIPLO DE ENTEROS

Observación: Dados dos números enteros a y b, el conjunto de los divisores comunes $D(a) \cap D(b)$ es un conjunto finito, luego tendrá un elemento máximo.

Definición: Se llama máximo común divisor de a y b y se representa por $M.C.D(a,b)$ al mayor elemento del conjunto $D(a)\cap D(b)$.

Nota: Para calcular el $M.C.D$ de dos números a y b se considera la descomposición en factores primos de ambos:

Sean $a=\alpha\cdot p_1^{\,n_1}\cdot p_2^{\,n_2}\cdots p_k^{\,n_k}$ y $b=\beta\cdot p_1^{\,m_1}\cdot p_2^{\,m_2}\cdots p_k^{\,m_k}$ y $d=M.C.D(a,b)$.

Para que d sea el máximo común divisor hace falta que sus exponentes sean menores o iguales que los de a y b y que sean lo más grandes posibles. Haciendo $r_i=\min(m_i,n_i)$ se tiene que $d=p_1^{\,r_1}\cdot p_2^{\,r_2}\cdots p_k^{\,r_k}$ y se concluye que $D(a)\cap D(b)=D(d)$.

Observación: Dados dos números enteros a y b el conjunto de los múltiplos positivos comunes $M^+(a)\cap M^+(b)$ es un subconjunto de los número naturales. Por el Principio de Buena Ordenación este conjunto tiene un elemento mínimo.

Definición: Se ***llama mínimo común múltiplo*** de a y b y se representa por $m.c.m(a,b)$ al elemento mínimo de $M^+(a)\cap M^+(b)$.

Nota: Análogamente al cálculo del $M.C.D(a,b)$ se tiene que el $m.c.m(a,b)$ se obtiene poniendo a los factores primos el mayor exponente de los que aparezcan.

Proposición:

Dados dos enteros a y b se tiene la igualdad $M.C.D(a,b)\cdot m.c.m(a,b)=|a\cdot b|$.

Demostración:

Sean $a=\alpha\cdot p_1^{\,n_1}\cdot p_2^{\,n_2}\cdots p_k^{\,n_k}$ y $b=\beta\cdot p_1^{\,m_1}\cdot p_2^{\,m_2}\cdots p_k^{\,m_k}$ con $\alpha,\beta=\pm1,\quad p_1,\cdots,p_k$ *primos*

Sean $r_i=\min(m_i,n_i)\ y\ s_i=\max(m_i,n_i)\ \forall i=1,\cdots,k\Rightarrow m_i+n_i=r_i+s_i$.

Entonces:

$$M.C.D(a,b)=p_1^{\,r_1}\cdot p_2^{\,r_2}\cdots p_k^{\,r_k};\ m.c.m(a,b)=p_1^{\,s_1}\cdot p_2^{\,s_2}\cdots p_k^{\,s_k}\Rightarrow$$
$$M.C.D(a,b)\cdot m.c.m(a,b)=p_1^{\,r_1+s_1}\cdot p_2^{\,r_2+s_2}\cdots p_k^{\,r_k+s_k}\Rightarrow$$
$$M.C.D(a,b)\cdot m.c.m(a,b)=p_1^{\,m_1+n_1}\cdot p_2^{\,m_2+n_2}\cdots p_k^{\,m_k+n_k}$$

Como $a\cdot b=\alpha\cdot\beta\cdot p_1^{\,m_1+n_1}\cdot p_2^{\,m_2+n_2}\cdots p_k^{\,m_k+n_k}=\alpha\cdot\beta\cdot M.C.D(a,b)\cdot m.c.m(a,b)$

Tomando valores absolutos se tiene el resultado:

$$|a\cdot b|=p_1^{\,m_1+n_1}\cdot p_2^{\,m_2+n_2}\cdots p_k^{\,m_k+n_k}=M.C.D(a,b)\cdot m.c.m(a,b)$$

Proposición: Identidad de Bezout

Sean $a,b\in Z$ y $d=M.C.D(a,b)$. Entonces $\exists m,n\in Z$ con $d=a\cdot m+b\cdot n$

Demostración:

Sea $H=\{a\cdot m+b\cdot n\,|\,m,n\in Z\ \ y\ \ a\cdot m+b\cdot n>0\}$. Sea x el mínimo de H

Como $d=M.C.D(a,b)\rightarrow\left\{\begin{matrix}d\,|\,a\rightarrow d\,|\,a\cdot m\\ d\,|\,b\rightarrow d\,|\,b\cdot n\end{matrix}\right\}\rightarrow d\,|\,a\cdot m+b\cdot n=x\overset{d,x>0}{\rightarrow}d\le x$.

Por otro lado, como $x,a\in Z\overset{\text{División Euclidea}}{\rightarrow}\exists k,r\ tal\ que\ a=k\cdot x+r\ con\ |r|<|x|$ y podemos además tomar $r\ge 0$. Como $x\in H, x=a\cdot m+b\cdot n$. Así, $r=a-k\cdot x\rightarrow$

$r=a-k\cdot(a\cdot m+b\cdot n)=a-k\cdot a\cdot m-k\cdot b\cdot n=a\cdot(1-km)+b\cdot(-kn)\rightarrow r=a\cdot m'+b\cdot n'$ Es decir, r tiene la forma de los elementos de H.

Pero como $|r|<|x|$ y $x=\min\{H\}\rightarrow r\notin H\rightarrow r=0\rightarrow a=k\cdot x$.

Análogamente podemos hacerlo con b.

Entonces tenemos que:

$$x\,|\,a\ \ y\ \ x\,|\,b\Rightarrow x\in D(a)\cap D(b)\Rightarrow x\le(D(a)\cap D(b))=d\Rightarrow x\le d$$

Luego $d=x=a\cdot m+b\cdot n$

Proposición: Sean $a,b,c\in Z$ con $a=b\cdot c+r$. Entonces: $M.C.D(a,b)=M.C.D(b,r)$.

Demostración: Bastará probar que $D(a)\cap D(b)=D(b)\cap D(r)$

$\subset)$ Sea $k\in D(a)\cap D(b)\rightarrow\left\{\begin{matrix}k\mid a\\ k\mid b\rightarrow k\mid b\cdot c\end{matrix}\right\}\rightarrow k\mid a-b\cdot c=r\Rightarrow$

$\Rightarrow k\mid r\Rightarrow k\in D(r)\overset{k\in D(b)}{\rightarrow}k\in D(b)\cap D(r)$

Como esto es cierto para cualquier elemento de $D(a)\cap D(b)$, se tiene que $D(a)\cap D(b)\subset D(b)\cap D(r)$.

$\supset)$ Sea ahora $k\in D(b)\cap D(r)\rightarrow\left\{\begin{matrix}k\mid b\rightarrow k\mid b\cdot c\\ k\mid r\end{matrix}\right\}\rightarrow k\mid b\cdot c+r=a\Rightarrow$

$\Rightarrow k\mid a\Rightarrow k\in D(a)\overset{k\in D(b)}{\rightarrow}k\in D(a)\cap D(b)$

Como esto es cierto para cualquier elemento de $D(b)\cap D(r)$, se tiene que $D(b)\cap D(r)\subset D(a)\cap D(b)$.

Luego: $D(b)\cap D(r)=D(a)\cap D(b)$.

Nota: Como $D(0)=Z$, se tiene que $D(a)\cap D(0)=D(a)\Rightarrow M.C.D(a,0)=a$.

Observación:

Resumiendo tenemos un procedimiento para calcular, M.C.D de dos números sin necesidad de hacer su descomposición factorial, se trata del algoritmo de Euclides:

- Se divide el mayor de los dos números entre el menor.
- Se divide el divisor de la división anterior entre el resto.
- Se repite la división entre el último divisor y el último resto hasta obtener resto cero.
- El máximo común divisor es el divisor de la última división.
- Para calcular el mínimo común múltiplo se multiplican los dos números y se divide el resultado entre el máximo común divisor calculado anteriormente.

Regla práctica: Calcular el $M.C.D(a,b)$ y el $m.c.m(a,b)$

cocientes	q_1	q_2	q_3	.....	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	.....	r_{n-2}	r_{n-1}	$r_n = MCD(a,b)$
r_1	r_2	r_3	r_4	.....	r_n	0	

$$m.c.m(a,b) = \frac{a \cdot b}{M.C.D(a,b)}$$

Ejemplo: $M.C.D(15,72)$ y $m.c.m(15,72)$

	4	1	4
72	15	12	3= $M.C.D(15,72)$
12	3	0	

$M.C.D(15,72) = 3$ y $m.c.m(15,72) = \frac{15 \cdot 72}{3} = 360$

3. CONGRUENCIAS

Definición: Sean $a,b \in Z$. Se dice que a es ***congruente*** con b módulo p, y se escribe $a \equiv b \pmod{p}$ si $p \mid a-b$.

Proposición:

a es congruente con b módulo p $\Leftrightarrow$ al dividir a y b entre p los restos resultantes son iguales.

Demostración:

$\Rightarrow)$ $a \equiv b \pmod{p}$. Dividiendo b entre p se tiene $b = c \cdot p + r$.

Pero como $a \equiv b \pmod{p}$ se tiene que $p \mid a-b \Rightarrow \exists k \in Z$ tal que:

$a - b = k \cdot p \Rightarrow a - (c \cdot p + r) = k \cdot p$.

Entonces: $a = b + (a-b) = c \cdot p + r + k \cdot p = (c+k) \cdot p + r$, luego al dividir a entre p se obtiene el mismo resto.

$\Leftarrow$) Supongamos ahora que en ambas divisiones se tiene el mismo resto:

$$\left.\begin{array}{l} a = p \cdot c + r \\ b = p \cdot c' + r \end{array}\right\} \Rightarrow a - b = (c - c') \cdot p \Rightarrow p \mid a - b \Rightarrow a \equiv b \pmod{p}$$

Proposición: La relación de congruencia es una relación de equivalencia.

Demostración:

Reflexiva: $\forall p \in Z : p \mid 0 = a - a \Rightarrow a \equiv a \pmod{p}$

Simétrica: Si $a \equiv b \pmod{p} \Rightarrow p \mid b - a \Rightarrow b \equiv a \pmod{p}$

Transitiva:

$$\left.\begin{array}{l} a \equiv b \pmod{p} \Rightarrow p \mid a - b \\ b \equiv c \pmod{p} \Rightarrow p \mid b - c \end{array}\right\} \Rightarrow p \mid (a-b) + (b+c) = a - c \Rightarrow a \equiv c \pmod{p}$$

Definición: El conjunto cociente se denota por $Z/(p)$.

Nota: Como todos los conjuntos cocientes está constituido por clases de equivalencia. Cada una de estas clase se representa escribiendo entre corchetes uno de los representantes. El representante más sencillo es el resto común de todas las divisiones entre p. Así, $Z/(p) = \{[0],[1],\cdots,[p-1]\}$, que es un conjunto formado por p elementos.

Definición: Se definen en $Z/(p)$ dos operaciones, que están bien definidas:

Suma: $[a] + [b] = [a+b]$

Producto: $[a] \cdot [b] = [a \cdot b]$

Nota: Con estas operaciones se verifican las propiedades de anillo conmutativo y unitario.

Proposición: Sea p un número entero no nulo. Entonces son equivalentes:

a) $Z/(p)$ es un cuerpo.

b) $Z/(p)$ es un dominio de integridad.

c) p es primo.

Demostración:

$a \Rightarrow b)$

Supongamos que $Z/(p)$ es un cuerpo, y sean $[a],[b] \in Z/(p)$ tales que $[a]\cdot[b]=[0]$.

Si $[a]\neq[0] \Rightarrow \exists[\dot{a}'] \in Z/(p) \; tal \; que \; [a']\cdot[a]=[1]$.

Entonces: $[b]=[1]\cdot[b]=[a']\cdot[a]\cdot[b]=[a']\cdot[0]=[0]$

$b \Rightarrow c)$

Supongamos ahora que $Z/(p)$ es un dominio de integridad y sea a un divisor de $p \Rightarrow \exists b \in Z$ con $p=a\cdot b$.

Pero $p \mid p = p-0 \rightarrow [0]=[p]=[a\cdot b]=[a]\cdot[b] \overset{Z/(p)\, es\, D.I}{\rightarrow} [a]=[0] \, ó \, [b]=[0]$

- Si $\left.\begin{matrix}[a]=[0]\rightarrow p \mid a-0=a \\ a \mid p\end{matrix}\right\} \rightarrow a=p,-p \rightarrow b=1,-1$.
- Si $\left.\begin{matrix}[b]=[0]\rightarrow p \mid b-0=b \\ b \mid p\end{matrix}\right\} \rightarrow b=p,-p \rightarrow a=1,-1$.

Luego p es primo.

$c \Rightarrow a)$ Supongamos que p es primo y sea $[a] \in Z/(p) \, tal \; que \, [a]\neq[0]$. Entonces p no divide a a. Luego $M.C.D(a,p)=1$. Por la Identidad de Bezout

$\exists m,n \in Z \; tal \; que \;\; a \cdot m + p \cdot n = 1 \rightarrow p \,|\, n \cdot p = 1 - a \cdot m \Rightarrow [1] = [a] \cdot [m] \Rightarrow \quad [m] \; inverso \; de \; [a]$. Luego $Z/(p)$ es un cuerpo.

Definición: Se llama ***i-ésimo resto potencial*** de b módulo p, al resto r_i que se obtiene al dividir b^i entre p.

Ejemplo: Los restos potenciales de 5 módulo 3 son:

5^0 | 3	5^1 | 3	5^2 | 3	5^3 | 3	5^4 | 3
1 0	2 1	1 8	2 41	1 208
$r_o = 1$	$r_1 = 2$	$r_2 = 1$	$r_3 = 2$	$r_4 = 1$

Propiedades: Los restos potenciales tienen las siguientes propiedades:

a) $r_0 = 1$

b) Si $r_i = 0 \Rightarrow r_{i+1} = 0$

c) $r_j = b \cdot r_{j-1} \pmod{p}$

d) Si $r_i = r_j \Rightarrow r_{i+k} = r_{j+k} \;\; \forall k \in \mathrm{N}$

Comentario:

La principal aplicación de la teoría de congruencia es su empleo en el estudio de la divisibilidad.

Evidentemente $p \,|\, n \Leftrightarrow [n] = [0] \; en \; Z/(p)$.

Dado el número $n = a_k a_{k-1} \cdots a_1 a_0$, expresado en base b, se trata de ver qué condiciones han de verificarse para que sea divisible por p.

$n = a_0 + a_1 \cdot b + \cdots + a_k \cdot b^k$ será múltiplo de p, si $[0] = [n] \; en \; Z/(p)$.

Tenemos que:

$$[n] = [a_0] + [a_1] \cdot [b] + \cdots + [a_k] \cdot [b^k] = [a_0] + [a_1] \cdot [r_1] + \cdots + [a_k] \cdot [r_k] = [a_0 + a_1 \cdot r_1 + \cdots + a_k \cdot r_k]$$

Entonces:

$$p \mid n \Leftrightarrow p \mid a_0 \cdot \underset{\downarrow}{r_0} + a_1 \cdot r_1 + \cdots + a_k \cdot r_k$$
$$1$$

Luego una vez calculados los restos potenciales bastará con aplicar la fórmula.

4. REGLAS DE DIVISIBILIDAD

Tomamos base decimal $(b=10)$ y veamos algunas reglas de divisibilidad entre p:

Sea $p=3$: En este caso: $r_0=1$; $r_1 \equiv 1\cdot 10 \equiv 1 \pmod 3$; como $r_0 = r_1 = 1 \Rightarrow r_j = 1 \ \ \forall j$.

Así, $3 \mid n \quad si \quad 3 \mid a_0 + a_1 + \cdots + a_k$.

Es decir, un número es múltiplo de 3 si lo es la suma de sus cifras.

Sea $p=5$: En este caso $r_0=1$; $r_1 \equiv 1\cdot 10 \equiv 0 \pmod 5$; como $r_1 = 0 \Rightarrow r_j = 0 \ \ \forall j \geq 1$.

Así, $5 \mid n \quad si \quad 5 \mid a_0$.

Es decir, un número es múltiplo de 5 si lo es su última cifra.

Sea $p=7$: En este caso $r_0=1$; $r_1 \equiv 1\cdot 10 \equiv 3 \pmod 7$; $r_2 \equiv 10\cdot 3 \equiv 2 \pmod 7$; $r_3 \equiv 10\cdot 2 \equiv 6 \equiv -1 \pmod 7$; $r_4 \equiv 10\cdot 6 \equiv 4 \equiv -3 \pmod 7$; $r_5 \equiv 10\cdot 4 \equiv 5 \equiv -2 \pmod 7$; $r_6 = 1$; como $r_6 = 1 = r_0 \Rightarrow r_{j+6} = r_j \ \ \forall j \geq 1$.

Así: $7 \mid n \quad si \quad 7 \mid a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - (a_9 + 3a_{10} + 2a_{11}) + \cdots$

5. CONCLUSIÓN

El estudio de la divisibilidad es muy importante, ya que es necesaria en múltiples áreas de las matemáticas, por ejemplo, el cálculo del mínimo común múltiplo de varios números es muy útil para poder sumar y restar fracciones con distinto denominador. ●

Bibliografía

Cohen, L.-Ehrlich, G.: The structure of the number systems.

Goldhaber, J.K.- Ehrlich,G.: Álgebra

Samuel, P.: Teoría algebraica de números.